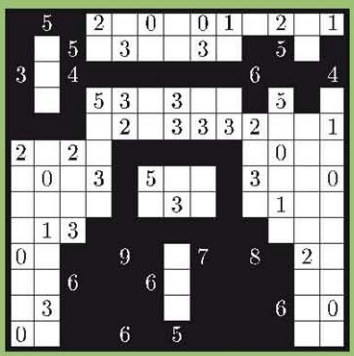
А. Ю. ЗУБОВ, А. В. ЗЯЗИН, Н. В. НИКОНОВ,
С. М. РАМОДАНОВ, А. А. ФРОЛОВ

ОЛИМПИАДЫ ПО КРИПТОГРАФИИ И МАТЕМАТИКЕ









А. Ю. Зубов, А. В. Зязин, Н. В. Никонов,
С. М. Рамоданов, А. А. Фролов

ОЛИМПИАДЫ ПО КРИПТОГРАФИИ И МАТЕМАТИКЕ ДЛЯ ШКОЛЬНИКОВ

Электронное издание

Москва
Издательство МЦНМО
2015

УДК 003.26
ББК 32.937-082.03
З91

Зубов А. Ю., Зязин А. В., Никонов Н. В., Рамоданов С. М.,
Фролов А. А.
Олимпиады по криптографии и математике для школьников.
Электронное издание
М.: МЦНМО, 2015
180 с.
ISBN 978-5-4439-2303-1

В сборник включены условия, ответы и решения двададцати олимпиад по криптографии и математике, проведенных в Москве с 1991/92 по 2010/11 уч. г. Условия задач предварены элементарным введением в криптографию, использующим сюжеты из известных литературных произведений.

Книга предназначена для учащихся старших классов, учителей математики и информатики, а также студентов младших курсов, интересующихся вопросами информационной безопасности.

Подготовлено на основе книги: *Зубов А. Ю.* и др. Олимпиады по криптографии и математике для школьников / А. Ю. Зубов, А. В. Зязин, Н. В. Никонов, С. М. Рамоданов, А. А. Фролов. — 2-е изд., перераб. и доп. — М.: МЦНМО, 2013.

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241-74-83
http://www.mccme.ru

© А. Ю. Зубов, А. В. Зязин, Н. В. Никонов,
С. М. Рамоданов, А. А. Фролов, 2015

ISBN 978-5-4439-2303-1 © МЦНМО, 2015

Предисловие

Эта книга имеет две основные цели. С одной стороны — дать популярное изложение основных понятий не всем хорошо известной и даже таинственной науки криптографии. Криптография возникла в глубокой древности первоначально как искусство защиты письменных сообщений. В настоящее время в развитых странах она является большой и сложной научно-технической областью деятельности, обеспечивающей защиту важной для государства как передаваемой по линиям связи, так и хранимой в файлах информации. С другой стороны, в книге обобщается многолетний опыт проведения Олимпиад для школьников по математике и криптографии и приводятся задачи, которые предлагались школьникам начиная с 1991 года. Задачи снабжены подробными решениями и ответами. Знакомство с этими задачами и их внимательный разбор могут помочь школьникам подготовиться и принять участие в Олимпиадах последующих лет. Книга написана квалифицированными математиками и криптографами и представляет значительный интерес как для школьников старших классов, так и для преподавателей математики в школе.

В современной криптографии проводятся глубокие научные исследования, опирающиеся на достижения математики, физики, информатики, электроники и теории связи. Традиционно особо тесную связь в этих исследованиях криптография имеет с математикой. Поэтому соединение в Олимпиадах задач по этим родственным дисциплинам является органичным и позволяет школьникам приобщиться к интересной области знаний и решению нестандартных задач, имеющих наряду с занимательной формой строгие математические постановки и нередко неожиданные оригинальные решения. Участие в Олимпиадах по математике и криптографии для учеников средней школы может послужить хорошим началом пути становления будущих специалистов в этих непростых, но увлекательных областях науки.

Юные участники и талантливые победители Олимпиад — это источник надежды, что через некоторое время в ряды отечественных криптографов и математиков вольются свежие силы, которые скажут новое слово в этих важных для нашей страны областях науки и техники.

Вице-президент Академии криптографии
Российской Федерации,
доктор физико-математических наук, профессор,
заслуженный деятель науки Российской Федерации

В. Н. Сачков

От авторов

С 1991/92 учебного года Академия криптографии Российской Федерации и Институт криптографии, связи и информатики Академии ФСБ России проводят ежегодную олимпиаду школьников по математике и криптографии для учащихся 8–11 классов. Олимпиада вызывает большой интерес у школьников необычностью своего жанра и уже с первых лет собирала несколько сотен участников из Москвы и Подмосковья.

С 2007/08 учебного года олимпиада стала межрегиональной. Благодаря помощи вузов, входящих в состав Учебно-методического объединения по образованию в области информационной безопасности, к настоящему времени очный тур проводится в более чем 30 регионах России, а участвуют в нём около 2000 школьников.

С 2008/09 года олимпиада по математике и криптографии ежегодно включается в Перечень олимпиад школьников, утверждаемый Министерством образования и науки России, что позволяет предоставлять льготы победителям и призёрам при поступлении в вузы.

Школьники часто спрашивают, с какой литературой по криптографии им следует ознакомиться, чтобы успешно выступить на олимпиаде. Никаких специальных знаний для решения задач не требуется — в этом вы убедитесь сами, ознакомившись с задачами, которые приводятся в этой книге. Вместе с тем мы не можем отрицать, что предварительное знакомство с криптографией полезно хотя бы с психологической точки зрения, поскольку «внешний вид» задач может показаться необычным. Многие задачи нашей олимпиады — криптографические. Часть задач имеют криптографическую окраску, но их суть — математическая. Отдельные задачи — просто математические.

Тематика предлагаемых задач весьма разнообразна. Задачи первых олимпиад в основном были посвящены так называемым ручным шифрам, некоторые из которых применялись ещё до нашей эры. Позднее появились задачи, в которых затрагиваются и разделы современной криптографии, такие как криптосистемы с открытым ключом и криптографические протоколы. Также возник цикл задач, относящихся скорее к области защиты информации, чем собственно к криптографии.

При составлении вариантов заданий олимпиады для различных возрастных категорий особое внимание уделяется оценке сложности задач и времени, отводимому на их решение. Благодаря этому практически каждый год находятся участники олимпиады, решившие все задачи.

При подведении итогов каждой олимпиады мы с удовлетворением отмечаем наличие в работах отдельных участников оригинальных решений, более красивых, чем исходно предполагавшиеся составителями.

Олимпиада имеет свой интернет-сайт `www.cryptolymp.ru`, на котором размещается информация о сроках и местах проведения туров олимпиады, результаты проверки прошедших туров, а также архив задач с решениями. На сайте размещаются методические материалы по математическим методам криптографии, специально адаптированные для школьников. Их цель — не только способствовать подготовке к успешному участию в олимпиаде, но и сформировать понимание математической сути задач защиты информации.

Мы считаем главной задачей олимпиады поддержание интереса школьников к математике, популяризацию её приложений, в первую очередь криптографии. Судя по количеству участников олимпиады в самых разных регионах России, нам это удаётся.

В последнее время книг по криптографии появилось достаточно много. Однако эти книги либо слишком сложны для школьников, либо, наоборот, поверхностны или недостаточно полны. Поэтому авторы при создании этой книги ставили перед собой две основные цели: во-первых, предложить элементарное введение в криптографию, используя при этом чудесные детективные сюжеты известных произведений Ж. Верна, А. Конан Дойла, Э. По, В. Каверина, связанные с зашифрованными сообщениями; во-вторых, привести условия задач всех наших олимпиад прошедших лет с ответами и решениями.

Представляя данную книгу, авторы считают своим долгом с благодарностью вспомнить своего коллегу и товарища П. А. Гырдымова (1954–2004), чей вклад в становление олимпиады по криптографии трудно переоценить. Авторы выражают также глубокую признательность всем своим коллегам, которые когда-либо предлагали готовые задачи и идеи новых задач, поддерживая тем самым саму олимпиаду, и энтузиазм её организаторов.

Работа над книгой выполнена при поддержке гранта Президента РФ (НШ-6260.2012.10).

1. Введение

Если вы хотите передать текстовое сообщение (последовательность символов некоторого алфавита) адресату так, чтобы оно осталось тайным для посторонних, то у вас есть по крайней мере две возможности. Вы можете попытаться скрыть сам факт передачи сообщения, то есть прибегнуть к методам стеганографии, в арсенале которой симпатические (невидимые) чернила, микроточки и тому подобные средства. Другая возможность заключается в таком преобразовании сообщения, зависящем от секретного параметра (называемого ключом), которое делает его «бессмысленным» набором символов для любого лица, которому ключ неизвестен. В этом случае вы будете использовать методы криптографии. Термин *криптография* происходит от двух греческих слов: *криптос* — тайна и *графейн* — писать, и означает тайнопись. «Тайнопись» как раз и подразумевает, что вы скрываете смысл сообщения.

В этой книге мы используем ряд других криптографических терминов. Вкратце поясним их.

Сообщение, которое вы хотите передать, будем называть *открытым сообщением* (или *открытым текстом*). Например, в задаче 2.5 (раздел «Условия задач») открытым сообщением является фраза

КОРАБЛИ ОТХОДЯТ ВЕЧЕРОМ

Для сохранения сообщения в тайне оно преобразуется криптографическими методами и только после этого передаётся адресату. Преобразованное сообщение будем называть *шифрованным сообщением* (или *шифртекстом*). Иногда шифртекст называют также *криптограммой*. В задаче 2.5 шифртекст имеет вид:

ЮПЯТБНЩМСДТЛЖГПСГХСЦЦ

Шифрованное сообщение не обязательно является последовательностью букв, как в указанной задаче. Оно может состоять из цифр или специальных символов (например, «пляшущих человечков»).

Преобразование открытого сообщения в шифрованное будем называть *шифрованием* или *зашифрованием*. Адресату заранее сообщается, как из шифртекста получить открытый текст. Это преобразование будем называть *расшифрованием*. Для расшифрования получателю необходимо знать секретный ключ. При выборе способа шифрования надо стремиться к тому, чтобы лица, не знающие секретного ключа, не смогли восстановить открытый текст по шифртексту, используя любые доступные средства. В этом случае вы скроете содержание сообщения и обеспечите «тайнопись».

Для удобства изложения введём ряд обозначений. Пусть A — открытый текст, B — шифртекст, E — правило зашифрования, D —

правило расшифрования. В этих обозначениях зашифрование запишется в виде $E(A) = B$, а расшифрование — в виде $D(B) = A$. Преобразования E и D должны быть взаимно обратными, чтобы получатель мог однозначно восстановить открытый текст по полученному шифртексту. Однотипные правила зашифрования объединяют в классы. Внутри класса правила различаются по значениям некоторого параметра, который может быть числом, строкой чисел, таблицей и т. д. В криптографии конкретное значение такого параметра и называют ключом. По сути дела, ключ выбирает конкретное правило зашифрования из данного класса правил.

Зависимость E от ключа k будем указывать в виде E_k, а соотношения, связывающие открытый и шифрованный тексты, — в виде $E_k(A) = B$ и $D_k(B) = A$ соответственно. Пусть K — множество возможных ключей. Тогда совокупность $\{(E_k, D_k) \colon k \in K\}$ будем называть *шифром*.

Среди всего множества шифров выделяют шифры перестановки и шифры замены. Шифры перестановки изменяют порядок следования символов открытого текста. При этом состав символов сообщения не изменяется. Например, можно поменять местами символы открытого текста, расположенные на чётных и нечётных местах. Шифры замены делят последовательность символов открытого текста на отрезки одинаковой длины l и заменяют каждый отрезок своим эквивалентом, последовательность которых образует шифртекст. При $l = 1$ шифр замены называется *поточным*, а при $l > 1$ — *блочным*. Например, у А. Конан Дойла каждый символ открытого текста заменяется «пляшущим человечком», то есть используется поточный шифр замены. Современные стандарты шифрования используют блочные шифры замены.

Как правило, в задачах наших олимпиад шифр известен, а использованный ключ — нет. В этом случае для определения открытого текста по шифртексту возможны два подхода. Первый — определить ключ и с его помощью произвести расшифрование. Второй — попытаться восстановить открытый текст без определения ключа. Говорят, что шифр удалось «взломать», если удалось восстановить открытый текст по шифртексту в случае, когда секретный ключ неизвестен. Чем сложнее взломать шифр, тем он более стоек. Некоторые (не очень стойкие) шифры удаётся взломать, что и демонстрируют победители наших олимпиад.

При анализе стойкости шифра обычно исходят из принципа, сформулированного голландцем Огюстом Керкгоффсом (1835–1903). Согласно этому принципу, стойкость шифрования определяется лишь секретностью ключа. Имеется в виду, что даже осведомлённый противник, которому всё известно о шифре, не может его взломать, если ему неизвестен ключ. Стойкий шифр должен иметь достаточно много

ключей, иначе его можно взломать путём перебора всех ключей. Этот метод используется, например, в задаче 4.4, решение которой сводится к перебору 24 возможных ключей, лишь один из которых даёт при расшифровании «читаемый» текст. Поэтому многие участники олимпиады смогли восстановить сообщение на латинском языке, даже не зная этого языка.

Подчас смешивают два понятия — *шифрование* и *кодирование*. Как вы уже поняли, методы шифрования используются для обеспечения секретности передаваемых сообщений. В свою очередь, методы кодирования широко используются в технике передачи сообщений по различным каналам связи. Так, при передаче информации по компьютерной сети удобно использовать кодирование символов сообщения двоичными наборами, например, байтами. Методы кодирования направлены не на то, чтобы скрыть открытое сообщение, а на то, чтобы представить его в более удобном виде для передачи по техническим каналам связи, например, для уменьшения длины сообщения и т. п. При передаче сообщений по радиоканалу используют азбуку Морзе, и так далее. Вместе с тем кодирование может использоваться и для обеспечения секретности информации. С этой целью можно закодировать, например, пятизначными комбинациями цифр часто используемые слова, фразы, некоторые комбинации букв, а также отдельные буквы. Полученный весьма объёмный код (совокупность цифровых комбинаций) должен быть секретным. Текст передаваемого сообщения может быть естественным образом закодирован с помощью такого кода и передан по каналу связи в виде цифровой последовательности. Такой способ может обеспечить секретность информации лишь до тех пор, пока не перестанет быть секретным сам код. Формально такой код можно рассматривать как шифр с одним ключом.

В настоящее время для защиты информации широко используются электронные шифровальные устройства. Их важной характеристикой является не только стойкость реализуемого шифра, но и высокая скорость шифрования и компактность. Такими устройствами может оснащаться не только военная техника, но и используемые в повседневной жизни пластиковые карты. Кроме аппаратных реализаций алгоритмов шифрования широкое распространение получили их программные реализации. Сегодня шифрование используется, например, для защиты электронной почты.

Современная криптография бурно развивается. Появляются её новые направления и приложения, основанные на глубоких математических и физических методах. Вы, наверное, слышали о «квантовой криптографии», использующей методы квантовой физики для распределения криптографических ключей, и о криптографии «с открытым

ключом», использующей для зашифрования и расшифрования разные ключи. Криптография с открытым ключом, основанная на классических теоретико-числовых и алгебраических методах, позволила решить проблему цифровой подписи электронных документов, а также целый ряд других проблем, которые не могли быть решены методами традиционной криптографии. К ним относятся многие *криптографические протоколы*, решающие важные практические задачи. Это, например, «бросание жребия по телефону», «доказательства с нулевым разглашением», проведение электронных торгов и электронного голосования и другие. Об этом вы можете почитать сегодня во многих книгах, посвящённых криптографии.

2. Шифры замены

Наибольшее распространение на практике получили шифры замены. Это объясняется простотой их использования и достаточной стойкостью. Они эффективно реализуются как аппаратно, так и программно. Многие задачи наших олимпиад посвящены именно шифрам замены.

Пусть, например, шифруется сообщение на русском языке и при этом замене подлежит каждая буква сообщения. В этом случае шифр замены можно описать следующим образом. Для каждой буквы α исходного алфавита выбирается некоторое множество символов M_α таким образом, что при $\alpha \neq \beta$ множества M_α и M_β не пересекаются. M_α назовём множеством *шифробозначений* для буквы α. Таблица

$а$	$б$	$в$	...	$я$
$M_а$	$M_б$	$M_в$	...	$M_я$

(1)

служит ключом шифра замены. Зная её, можно осуществить как зашифрование, так и расшифрование. При зашифровании каждая буква α открытого текста заменяется любым символом из множества M_α. Если в сообщении содержится несколько букв α, то каждая из них заменяется любым символом из M_α. За счёт этого можно с помощью одного ключа (1) получить различные варианты зашифрования данного сообщения. Например, если ключом является таблица

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

то сообщение «я знаком с шифрами замены» может быть зашифровано любым из следующих способов:

16 55 54 10 69 09 61 89 29 90 49 44 10 08 02 73 21 32 83 54 74
41 55 77 10 23 68 08 20 66 90 76 44 21 61 90 55 21 61 83 54 42
57 30 27 10 91 68 32 20 80 02 49 45 40 32 46 55 40 08 83 27 42

Так как множества $M_а$, $M_б$, $M_в$, ..., $M_я$ попарно не пересекаются, по каждому символу шифртекста можно однозначно определить, какому множеству он принадлежит, то есть какую букву открытого текста он заменяет. Поэтому расшифрование возможно, и открытый текст определяется единственным образом.

Множества M_α состоят в большинстве случаев из одного элемента. Например, в романе Ж. Верна «Путешествие к центру Земли» в руки профессора Лиденброка попадает пергамент с рукописью из знаков рунического письма. Каждое множество M_α состоит из одного элемента. Элемент каждого множества выбирается из набора символов вида



(2)

В рассказе А. Конан Дойла «Пляшущие человечки» каждый символ изображает пляшущего человечка в самых различных позах



(3)

На первый взгляд кажется, что чем «хитрее» символы, используемые в качестве шифробозначений, тем сложнее найти открытый текст, не имея ключа. Это, конечно, не так. Можно легко перейти от исходного шифртекста к шифртексту, состоящему из букв или чисел, заменив ими «хитрые» символы. Так герои романа Ж. Верна «Путешествие к центру Земли» заменили рунические символы буквами немецкого алфавита, и это облегчило получение открытого текста.

Рассмотрим примеры шифров замены.

Пусть каждое множество M_α состоит из одной буквы (такой шифр называется шифром *простой однобуквенной замены*). Например,

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
г	л	ь	п	д	р	а	м	ц	в	э	ъ	х	о	б	н

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
с	ж	я	и	ю	к	щ	ф	е	у	ы	ч	ш	т	а

(4)

Ключ (4) удобно использовать для шифрования. При зашифровании каждая буква открытого текста ищется в верхней строке таблицы и заменяется расположенной под ней буквой второй строки. Расшифрование производится в обратном порядке. По сути дела, в приведённом приме-

ре ключом служит вторая строка таблицы (4), представляющая собой перестановку букв алфавита. Из истории криптографии известен ряд способов, позволяющих легко восстанавливать такие перестановки на основе некоторого простого правила. Это необходимо для того, чтобы исключить потерю ключа, записанного, например, на листе бумаги.

Одним из старейших шифров является шифр Цезаря. Это шифр простой однобуквенной замены, ключом которого служит таблица (4), вторая строка которой является циклическим сдвигом первой строки. Одним из ключей такого шифра является, например, таблица

а	б	в	...	ь	э	ю	я
г	д	е	...	я	а	б	в

(5)

Для восстановления такого ключа нужно знать лишь первую букву второй строки. Однако это удобство имеет и противоположную сторону: число ключей шифра Цезаря равно числу букв алфавита, и не представляет труда все их перебрать, чтобы определить истинный ключ по данной криптограмме путём расшифрования. Задача 4.4, например, именно на это и рассчитана. В одном из вариантов расшифрования участники олимпиады смогли узнать «читаемый» текст на латинском языке.

Другой пример шифра простой замены — так называемый *лозунговый шифр*. Для этого шифра вторая строка таблицы(4) начинается с легко запоминаемого слова — лозунга. Остальные буквы алфавита, не входящие в лозунг, следуют в их естественном порядке. Такую перестановку букв алфавита называют систематически перемешанным алфавитом. Выбрав, например, в качестве лозунга слово «учебник», получим систематически перемешанный алфавит

у	ч	е	б	н	и	к	а	в	г	д	ж	з	л	м	о
п	р	с	т	ф	х	ц	ш	щ	ъ	ы	ь	э	ю	я	

Число ключей лозунгового шифра значительно больше, чем у шифра Цезаря.

Шифры простой однобуквенной замены имеют одну общую слабость. Заметим, что если в открытом тексте часто встречается какая-либо буква, то в шифртексте столь же часто встречается заменяющий её символ. То же касается и редких букв. Если имеется шифртекст достаточной длины, то указанное соответствие несложно использовать при идентификации букв открытого текста, даже если ключ неизвестен. В некоторых задачах олимпиад такая идентификация упрощается путём введения дополнительных условий. Например, в задаче 4.2 при шифровании сохранена разбивка текста на слова и указаны знаки препинания. Это позволяет выделить предлоги и союзы. Кроме того, текст сообщения содержит ряд удвоенных букв, которым скорее всего в открытом тексте соответствуют один из вариантов: НН, ОО, ИИ

и т. д. Если правильно идентифицированы несколько букв открытого текста (например, ряд частых букв), то дальнейшая работа по определению ключа не представляет особого труда. Решение подобных задач достаточно сложно формализовать, и в таких случаях уместно вспомнить высказывание о том, что криптография не только наука, но и искусство.

Популярные среди школьников криптограммы (типа криптограммы из задачи 1.5) фактически связаны с простой заменой, пределяемой ключом

0	1	2	3	4	5	6	7	8	9
ш	и	ф	р	э	а	м	е	н	ы

в котором каждая цифра заменяется буквой. При этом должны соблюдаться правила арифметики. Эти правила значительно облегчают решение задачи, так же как правила русского языка облегчают в задаче 4.2 нахождение четверостишия В. Высоцкого.

Любые особенности текста, которые могут быть вам известны, — ваши помощники. Например, в задаче 5.2 прямо указано, что в тексте используются телеграфные сокращения «зпт» и «тчк». И эта подсказка указывает путь к решению задачи.

Одной из разновидностей шифров простой замены являются шифры *разнозначной замены*, заменяющие каждую букву одним или двумя символами (как в задаче 4.2). Например, ключ такого шифра задаётся таблицей

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
73	74	51	65	2	68	59	1	60	52	75	61	8	66	58	3

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
69	64	53	54	9	62	71	4	67	56	72	63	55	70	57

Если шифртекст записан без знаков пробела, то при анализе шифра разнозначной замены появляется дополнительная трудность, связанная с разбиением сообщения на отдельные символы и слова. Взломать такой шифр сложнее, нежели шифр простой однобуквенной замены.

Другое усложнение шифра простой замены состоит в том, чтобы множества шифробозначений M_α содержали более одного элемента. Такие шифры получили название шифров *многозначной замены* (или *омофонов*). Эти шифры позволяют скрыть истинную частоту букв открытого текста, что существенно затрудняет их анализ. Однако при использовании омофонов возникает сложность, связанная с хранением ключа. Ключ представляет собой список множеств M_α для каждой буквы алфавита. Как правило, элементами этих множеств являются числа.

Пример омофона известен из художественной литературы и кинофильмов про разведчиков времён Второй мировой войны. Это — одна

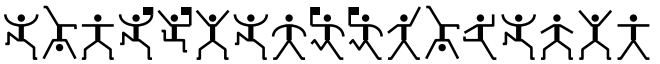
из разновидностей так называемого *книжного шифра*. Ключом шифра служит книга. Множество шифробозначений для каждой буквы определяется пятизначными наборами цифр, в которых первые две цифры указывали номер страницы, третья цифра — номер строки, четвёртая и пятая цифры — номер позиции буквы в строке. Поэтому при поимке разведчика, который пользовался таким шифром, всегда пытались найти книгу, которая могла быть использована им в качестве ключа.

Мы не касаемся в нашем кратком введении более сложных методов построения шифров замены. Полагаем, что приведённых примеров достаточно для того, чтобы оценить многообразие шифров. Закончим рассказ о шифрах замены несколькими красивыми примерами, заимствованными из художественной литературы.

А. Конан Дойл, «Пляшущие человечки»

В этом рассказе Холмсу необходимо было прочитать тексты пяти записок:

I. 

II. 

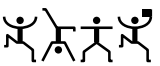
III. 

IV. 

V. 

Первая записка была так коротка, что дала возможность Холмсу сделать всего лишь одно правдоподобное предположение, оказавшееся впоследствии правильным. По-видимому, флаги употребляются лишь для того, чтобы отмечать концы отдельных слов. Больше ничего по первой записке установить было нельзя. Четвёртая записка, по всей видимости, содержала всего одно слово, так как в ней не было флагов.

Вторая и третья записки начинались, несомненно, с одного и того же слова из четырёх букв. Вот это слово:



Оно кончается той же буквой, какой и начинается. Счастливая мысль: письма обычно начинаются с имени того, кому письмо адресовано. Человек, писавший миссис Кьюбит эти послания, был, безусловно, близко

с ней знаком. Вполне естественно, что он называет её просто по имени. А зовут её Илси. Таким образом, Холмсу стали известны три буквы: И, Л и С.

В двух записках их автор обращается к миссис Кьюбит по имени и, видимо, чего-то требует от неё. Не хочет ли он, чтобы она пришла куда-нибудь, где он мог с ней поговорить? Холмс обратился ко второму слову третьей записки. В нём 7 букв, из которых третья и последняя — И. Холмс предположил, что слово это — ПРИХОДИ, и сразу оказался обладателем ещё 5 букв: П, Р, Х, О, Д.

Тогда он обратился к четвёртой записи, которая появилась на двери сарая. Холмс предположил, что она является ответом и что написала её миссис Кьюбит. Подставив в текст уже известные буквы, он получил: -И-О-Д-. Что же могла миссис Кьюбит ответить на просьбу прийти? Внезапно Холмс догадался: НИКОГДА

Возвратившись к первой записке, Холмс получил:

\- -Д-С- А- СЛ-НИ

Он предположил, что четвёртое слово — СЛЕНИ Это — фамилия, чрезвычайно распространённая в Америке. Коротенькое слово из двух букв, стоящее перед фамилией, по всей вероятности, имя. Какое же имя может состоять из двух букв? В Америке весьма распространено имя Аб. Теперь остаётся установить только первое слово фразы; оно состоит всего из одной буквы, и отгадать его нетрудно: это — местоимение Я.

Далее Холмс восстанавливает содержание второй записки:

```
ИЛСИ  Я   -И- -   -  -ЛРИД-А
          *  o   o       *
```

Здесь указаны границы слов, а снизу одинаковыми символами отмечены одинаковые буквы. Четвёртое слово состоит из одной буквы (по-видимому, это союз или предлог). Буквы О и И уже определены, С, А и К — тоже. Остаются следующие возможности: это — либо В, либо У. Вряд ли это — В, так как в этом случае получилось бы «нечитаемое» третье слово -И-В. Поэтому, скорее всего — это предлог У. Небольшой перебор незадействованных букв даёт правдоподобную гипотезу о значении третьего слова: ЖИВУ. Скорее всего, последнее слово (-ЛРИДЖА) — мужское имя, в котором неизвестная буква — Э. Поэтому вторая записка гласит:

ИЛСИ Я ЖИВУ У ЭЛРИДЖА

Холмс послал телеграмму в нью-йоркское полицейское управление с запросом о том, кто такой Аб Слени. Поступил ответ: «Самый опасный бандит в Чикаго».

Сразу после этого появилась последняя (5-я) записка, в которой не хватало трёх букв: ИЛСИ ГО-ОВЬСЯ К С-ЕР-И, из которой сразу опреде-

ляются буквы M и T:

ИЛСИ ГОТОВЬСЯ К СМЕРТИ

Шестая записка была направлена Холмсом преступнику:



Э. По, «Золотой жук»

Найден пергамент с текстом криптограммы. Для удобства пронумеруем по порядку все символы этого текста:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5	3	#	#	+	3	0	5	)	)	6	*	;	4	8	2	6	)	4
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36		
#	•	)	4	#	)	;	8	0	6	*	;	4	8	+	8	□		
37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52			
6	0	)	)	8	5	;	;	]	8	*	;	:	#	*	8			
53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69		
+	8	3	(	8	8	)	5	*	+	;	4	6	(	;	8	8		
70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86		
*	9	6	*	?	;	8	)	*	#	(	;	4	8	5	)	;		
87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102			
5	*	+	2	:	*	#	(	;	4	9	5	6	*	2	(			
103	104	105	106	107	108	109	110	111	112	113	114	115						
5	*	=	4	)	8	□	8	*	;	4	0	6						
116	117	118	119	120	121	122	123	124	125	126	127	128						
9	2	8	5	)	;	)	6	+	8	)	4	#						
129	130	131	132	133	134	135	136	137	138	139	140	141	142					
#	;	1	(	#	9	;	4	8	0	8	1	;	8					
143	144	145	146	147	148	149	150	151	152	153	154	155	156					
:	8	#	1	;	4	8	+	8	5	;	4	)	4					
157	158	159	160	161	162	163	164	165	166	167	168	169						
8	5	+	5	2	8	8	0	6	*	8	1	(						
170	171	172	173	174	175	176	177	178	179	180	181	182						
#	9	;	4	8	;	(	8	8	;	4	(	#						
183	184	185	186	187	188	189	190	191	192	193	194	195						
?	3	4	;	4	8	)	4	#	;	1	6	1						
196	197	198	199	200	201	202	203	204										
;	:	1	8	8	;	#	?	;										

Кроме того, на пергаменте изображены череп и козлёнок. Главный герой рассказа рассуждал следующим образом. По английски козлёнок — kid; череп связан с капитаном Киддом, по английски — kidd. Козлёнок

Содержание

Предисловие 3
От авторов 4
1. Введение 6
2. Шифры замены 9
3. Шифры перестановки 21
4. Многоалфавитные шифры замены 29
5. Современные приложения криптографии 32
6. Условия задач олимпиад по криптографии и математике 36
7. Указания и решения 75
Рекомендуемая литература 179